

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

LISTING OF CLAIMS:

1. (Currently amended) ~~A~~An apparatus for detecting adversarial activity on a network, comprising:
 - a memory adapted to store a host table;
 - a key exchanger adapted to derive a cipher key;
 - a translator adapted to translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include an address;
 - a mapping device adapted to map the address to the host table;
 - a host resolution device adapted to issue a request to the network to resolve the address when the address does not match an entry in the host table and to supplement the host table with the address upon receipt of a reply to the request that indicates that the address is valid; and
 - an actuator adapted to trigger a security device when the address does not match an entry in the host table.
2. (Original) An apparatus as set forth in Claim 1, wherein the security device is a logging device adapted to log the data packet.
3. (Original) An apparatus as set forth in Claim 1, wherein the security device is adapted to signal an alarm when triggered.
4. (Currently amended) An apparatus as set forth in Claim 1, wherein said host resolution device is adapted to derive the host table using an address resolution protocol.

5. (Original) An apparatus as set forth in Claim 1, further comprising:
a network device adapted to place the data packet onto a network when the address maps to the host table.
6. (Previously presented) A method for detecting adversarial activity on a network, comprising:
storing a host table;
deriving a cipher key;
translating predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include an address;
mapping the address to the host table;
issuing a request to the network to resolve the address when the address does not match an entry in the host table and supplementing the host table with the address upon receipt of a reply to the request that indicates that the address is valid; and
triggering a security device when the address does not match an entry in the host table.
7. (Original) A method as set forth in Claim 6, further comprising:
logging the data packet when the address does not match an entry in the host table.
8. (Original) A method as set forth in Claim 6, further comprising:
signaling an alarm when the security device is triggered.
9. (Previously presented) A method as set forth in Claim 6, further comprising:
deriving the host table using an address resolution protocol.
10. (Original) A method as set forth in Claim 6, further comprising:

placing the data packet onto a network when the address maps to the host table.

11. (Previously presented) A device for detecting adversarial activity on a network, comprising:

means for storing a host table;

means for deriving a cipher key;

means for translating predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include an address;

means for mapping the address to the host table;

means for issuing a request to the network to resolve the address when the address does not match an entry in the host table and supplementing the host table with the address upon receipt of a reply to the request that indicates that the address is valid; and

means for triggering a security device when the address does not match an entry in the host table.

12. (Original) A device as set forth in Claim 11, further comprising:

means for logging the data packet when the address does not match an entry in the host table.

13. (Original) A device as set forth in Claim 11, further comprising:

means for signaling an alarm when the security device is triggered.

14. (Previously presented) A device as set forth in Claim 11, further comprising:

means for deriving the host table using an address resolution protocol.

15. (Original) A device as set forth in Claim 11, further comprising:

means for placing the data packet onto a network when the address maps to the host table.

16. (Previously presented) A bastion host adapted for processing packet header information of a data packet, the bastion host being operable to:
- store a host table;
 - derive a cipher key;
 - translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include an address;
 - map the address to the host table;
 - issuing a request to the network to resolve the address when the address does not match an entry in the host table and supplement the host table with the address upon receipt of a reply to the request that indicates that the address is valid; and
 - trigger a security device when the address does not match an entry in the host table.
17. (Original) The bastion host as set forth in Claim 16, the bastion host being further operable to log the data packet when the address does not match an entry in the host table.
18. (Original) The bastion host as set forth in Claim 16, the bastion host being further operable to signal an alarm when the security device is triggered.
19. (Previously presented) The bastion host as set forth in Claim 16, the bastion host being further operable to derive the host table using an address resolution protocol.
20. (Original) The bastion host as set forth in Claim 16, the bastion host being further operable to place the data packet onto a network when the address maps to the host table.

21. (Previously presented) An apparatus as set forth in Claim 1, wherein said key exchanger is further adapted to repeatedly derive a cipher key with the cipher key derived by said key exchanger changing over time.

22. (Previously presented) A method as set forth in Claim 6, wherein deriving the cipher key comprises repeatedly deriving a cipher key such that the resulting cipher key changes over time.

23. (Previously presented) A device as set forth in Claim 11, wherein said means for deriving a cipher key is further adapted to repeatedly derive a cipher key such that the resulting cipher key changes over time.

24. (Previously presented) A bastion host as set forth in Claim 16, the bastion host being further operable to repeatedly derive a cipher key such that the resulting cipher key changes over time.